Wireless Protocols for IoT Part III: Zigbee

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

These slides and audio/video recordings of this class lecture are at:
http://www.cse.wustl.edu/~jain/cse574-20/

Student Questions

Overview

1. Zigbee Features, Versions, Device Types, Topologies
2. Zigbee Protocol Architecture
3. Zigbee Application, Zigbee Application Support Layer
4. Network Layer, Routing: AODV, DSR
5. Zigbee Smart Energy V2

Note: This is the 3rd lecture in series of class lectures on IoT. Bluetooth, Bluetooth Smart, IEEE 802.15.4 were covered in the previous lectures..

Student Questions

Zigbee PRO Features

- Zigbee PRO: Published in 2007.
- **Stochastic addressing**: A device is assigned a random address and announced. Mechanism for address conflict resolution. Parents don't need to maintain assigned address table.
- **Link Management**: Each node maintains quality of links to neighbors. Link quality is used as link cost in routing.
- **Frequency Agility**: Nodes experience interference report to channel manager (e.g., trust center), which then selects another channel
- **Multicast**
- **Many-to-One Routing**: To concentrator
- **Asymmetric Link**: Each node has different transmit power and sensitivity. Paths may be asymmetric.
- **Fragmentation** and Reassembly

Student Questions

- In a concentrator like an coordinator?

Yes and no. Some applications (not all) have n-to-1 traffic. In those cases, the central point is called a concentrator.

Zigbee Overview

- Industrial monitoring and control applications requiring small amounts of data, turned off most of the time (<1% duty cycle), e.g., wireless light switches, meter reading, patient monitoring
- First standard was published in 2004
- Ultra-low power, low-data rate, multi-year battery life
- Power management to ensure low power consumption.
- Less Complex. 32kB protocol stack vs 250kB for Bluetooth
- **Range**: 1 to 100 m, up to 65000 nodes.
- **Tri-Band**:
  - 16 Channels at 250 kbps in 2.4GHz ISM
  - 10 Channels at 40 kb/s in 915 MHz ISM band (Americas)
  - One Channel at 20 kb/s in European 868 MHz band
  - 920 MHz in Japan

Student Questions

Zigbee Overview (Cont)

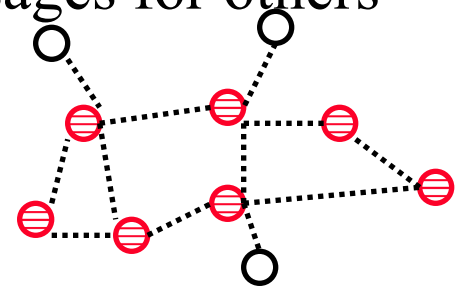
- IEEE 802.15.4 MAC and PHY
  (Except for Zigbee Smart Energy 2.0)
  Higher layer and interoperability by Zigbee Alliance
- Up to 254 devices or 64516 (~2^{16}) simpler nodes
- Named after zigzag dance of the honeybees
  Direction of the dance indicates the location of food
- Multi-hop ad-hoc mesh network

Multi-Hop Routing: message to non-adjacent nodes

Ad-hoc Topology: No fixed topology. Nodes discover each other

Mesh Routing: End-nodes help route messages for others

Mesh Topology: Loops possible



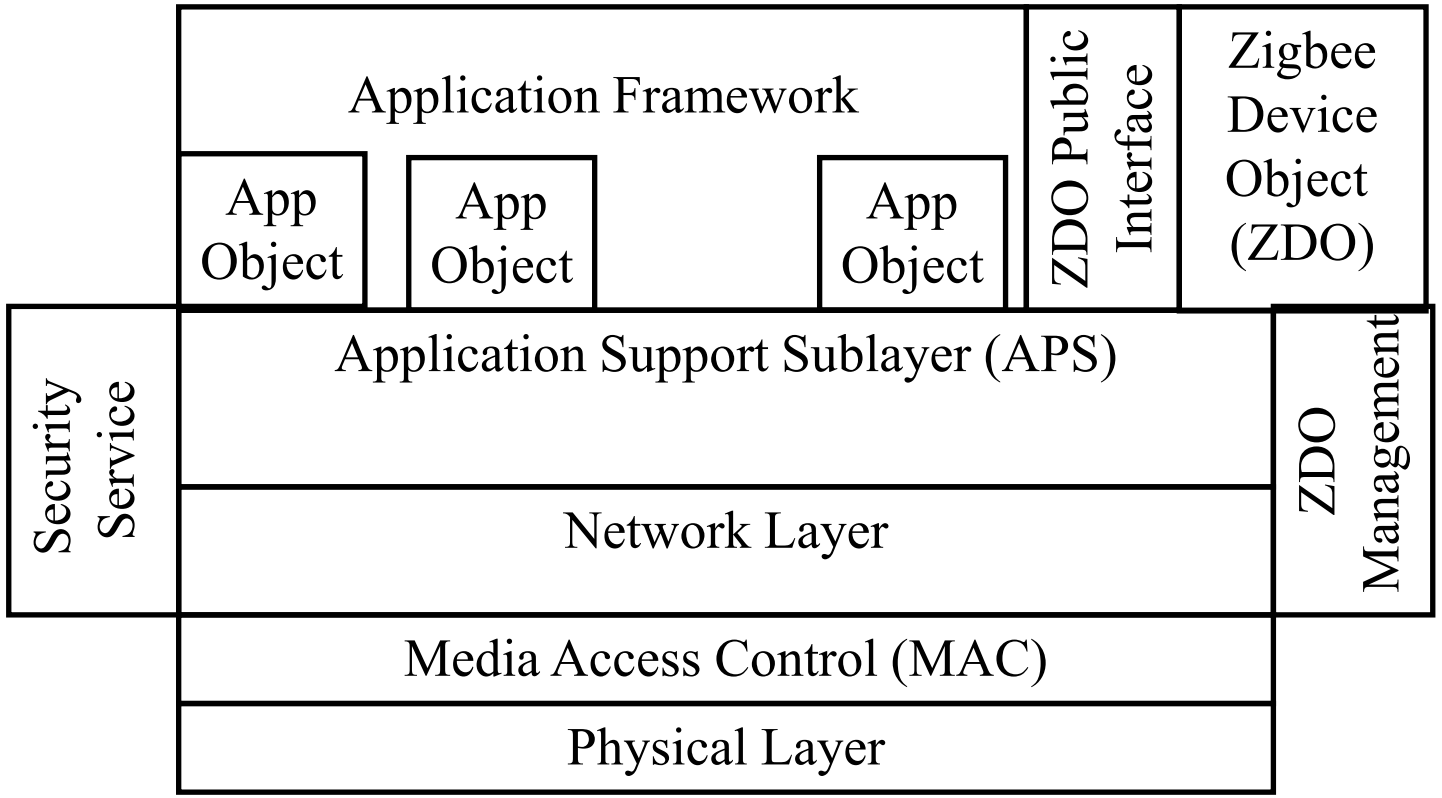
Ref: Zigbee Alliance, http://www.Zigbee.org

Student Questions

- Could you go over the difference between mesh topology and router again? I'm more confused on the idea of mesh topology.

Mesh routing means "end-nodes" do the routing. For example, you may forward your neighbor's packets to them. This has not been successful due to economic considerations. What's in it for me? Mesh topology is as shown. Some nodes are end nodes and some are intermediate nodes. This is quite common.

Zigbee Protocol Architecture



Student Questions

PRO Features (Cont)

- **Power Management**: Routers and Coordinators use main power. End Devices use batteries.
- **Security**: Standard and High
  End-Devices get new security key when they wake up.
- **Backward Compatible**:
  - Pro-devices act as non-routing Zigbee end devices (ZEDs) on legacy Zigbee network.
  - Legacy Zigbee devices act as non-routing Zigbee end-devices on Zigbee Pro Network

Student Questions

- Why do routers need main power? Is this because they need to be on all the time?

Yes, Exactly.

Zigbee Device Types

- **Coordinator**: Selects channel, starts the network, assigns short addresses to other nodes, transfers packets to/from other nodes
- **Router**: Transfers packets to/from other nodes
- **Full-Function Device**: Capable of being coordinator or router
- **Reduced-Function Device**: Not capable of being a coordinator or a router ⇒ Leaf node
- **Zigbee Trust Center (ZTC):** Provides security keys and authentication
- **Zigbee Gateway**: Connects to other networks, e.g., WiFi

Student Questions

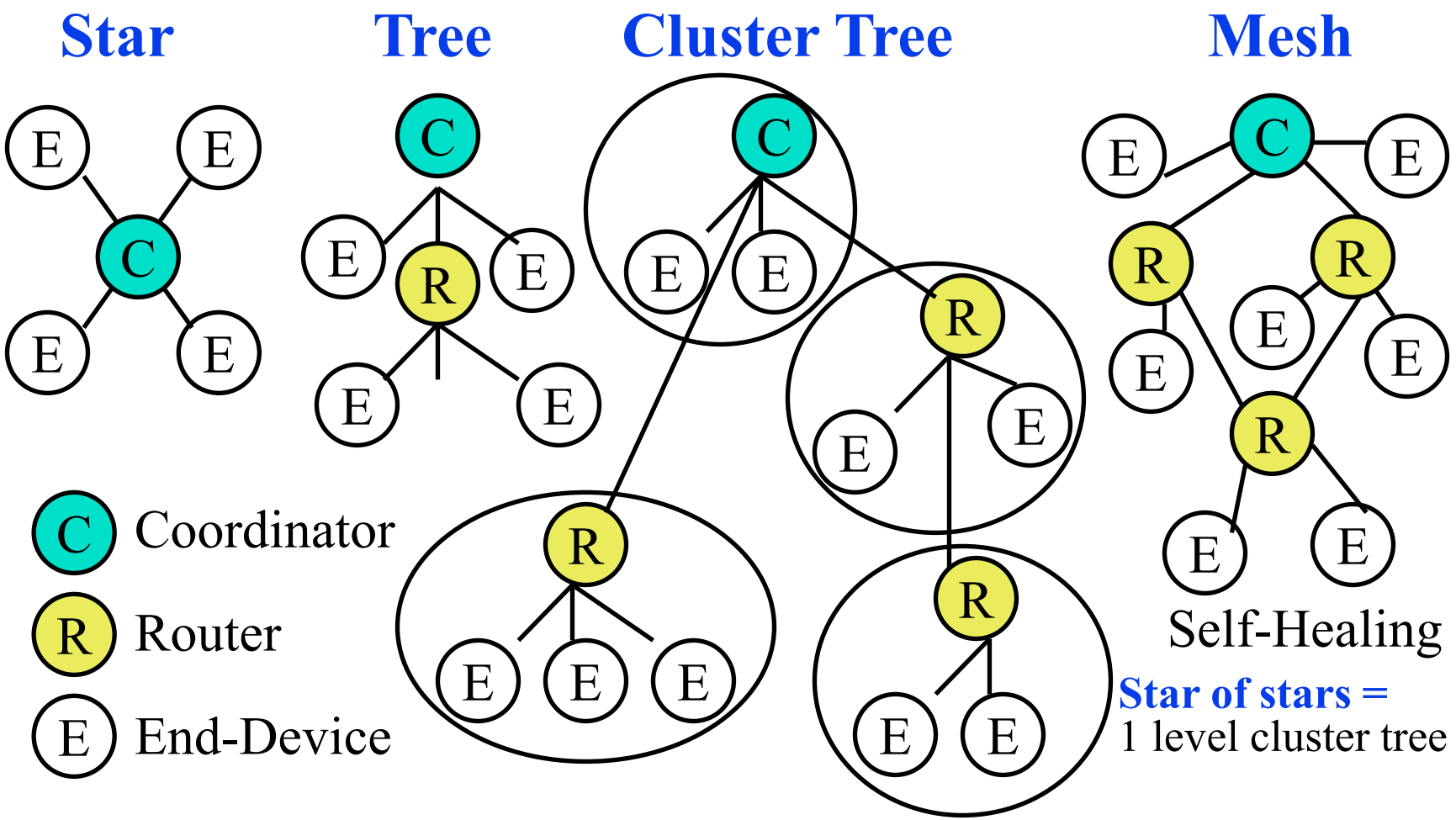
- So only Reduced-Function devices can use batteries in pro- devices?

RFD's can use main's power or battery depending upon their location. By they way, non-RFDs are not prohibited from using batteries. But you will need big batteries to support the power requirements.

- Does the ZTC exist outside of the hub//gateway?

It is a function. Not a box. Functions can reside in any box. Most boxes implement more than one function. ZTC can reside in the hub or in the cloud.

Zigbee Topologies



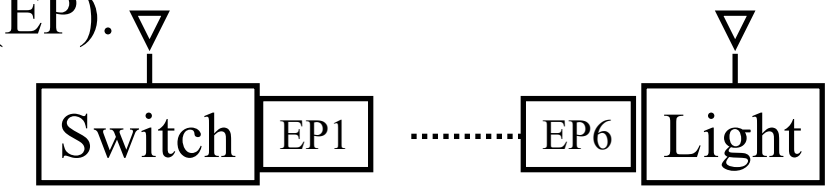
Student Questions

- How is a topology decided on?

Decided by the users and manufacturers. Some users don't like trees (no redundancy). Some don't like mesh (looping). Some manufacturers may not support complicated (mesh) routing to keep costs down.

Zigbee Protocol Architecture (Cont)

- **Application Objects**: e.g., Remote control application. Also referred to as **End-Point** (EP).



- **End-Node**: End device. Each node can have up to 250 application objects.
- **Zigbee Device Object (ZDO)**: Control and management of application objects. Initializes coordinator, security service, device and service discovery
- **Application Support Layer (APS)**: Serves application objects.
- **Network Layer**: Route Discovery, neighbor discovery
- ZDO Management
- Security Service

Student Questions

Zigbee Application Layer

- Application layer consists of application objects (aka end points) and Zigbee device objects (ZDOs)
- 256 End Point Addresses:
  - 240 application objects: Address EP1 through EP240
  - ZDO is EP0
  - End Points 241-254 are reserved
  - EP255 is broadcast
- Each End Point has one application profile, e.g., light on/off profile
- Zigbee forum has defined a number of profiles.
  Users can develop other profiles
- **Attributes**: Each profile requires a number of data items. Each data item is called an "attribute" and is assigned an 16-bit "attribute ID" by Zigbee forum

Student Questions

- What are endpoints 241-254 reserved for?

Future use

Zigbee Application Layer (Cont)

- **Clusters**: A collection of attributes and commands on them. Each cluster is represented by a 16-bit ID. Commands could be read/write requests or read/write responses
- **Cluster Library**: A collection of clusters. Zigbee forum has defined a number of cluster libraries, e.g., General cluster library contains on/off, level control, alarms, etc.
- **Binding**: Process of establishing a logical relationship (parent, child, ..)
- **ZDO**:
  - Uses device and service discovery commands to discover details about other devices.
  - Uses binding commands to bind and unbind end points.
  - Uses network management commands for network discover, route discovery, link quality indication, join/leave requests

Student Questions

- Does a device implement a set of clusters?

Yes.

Zigbee Application Profiles

- **Smart Energy**: Electrical, Gas, Water Meter reading
- **Commercial Building Automation**: Smoke Detectors, lights, …
- **Home Automation**: Remote control lighting, heating, doors, …
- **Personal, Home, and Hospital Care (PHHC)**: Monitor blood pressure, heart rate, …
- **Telecom Applications**: Mobile phones
- **Remote Control for Consumer Electronics**: In collaboration with Radio Frequency for Consumer Electronics (RF4CE) alliance
- **Industrial Process Monitoring and Control**: temperature, pressure, position (RFID), …
- Many others

Ref: A. Elahi and A. Gschwender, "Zigbee Wireless Sensor and Control Network," Prentice Hall, 2009, 288 pp., ISBN:0137134851, Safari Book

Student Questions

Sample Zigbee Products

Lock
(Kwikset)

Light Bulb
(Sengled)

Hub
(Samsung)

Motion Detector
(Bosch)

Outlet
(Samsung)

Temperature Sensor
(Visonic)

Student Questions

- Phillips Hue smart lightbulb devices are moving away from requiring a hub. Does this mean that devices like this are moving away from Zigbee or are connecting in a different way?

Yes. Wi-Fi with existing access points or APs built-in the bulbs can do the same job cheaply.

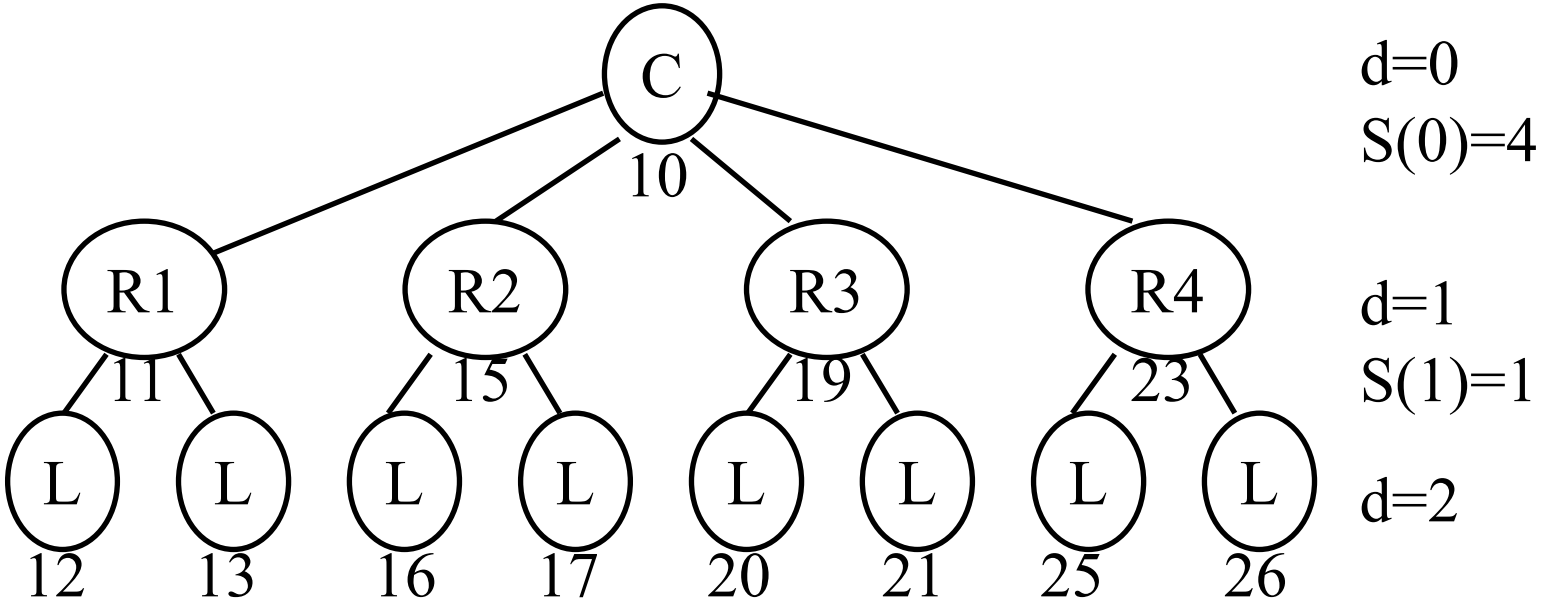
Zigbee Address Assignment

- Each node gets a unique 16-bit address
- Two Schemes: Distributed and Stochastic
- Distributed Scheme: Good for tree structure
  - Each child is allocated a sub-range of addresses.
  - Need to limit maximum depth L, Maximum number of children per parent C, and Maximum number of routers R
  - Address of the n^{th} child is parent+(n-1)S(d)

$$S(d) = \begin{cases} 1 + C(L-d) & \text{if } R = 1 \\ \frac{CR^{L-d-1} - 1 - C + R}{R-1} & \text{if } R > 1 \end{cases}$$

Student Questions

Distributed Scheme Example



- Max depth L=2, Routers R=4, Children C=3
- Coordinator: d=0. Skip

$$S(0) = \frac{CR^{L-d-1} - 1 - C + R}{R - 1} = \frac{3 \times 4^{2-0-1} - 1 - 3 + 4}{4 - 1} = 4$$

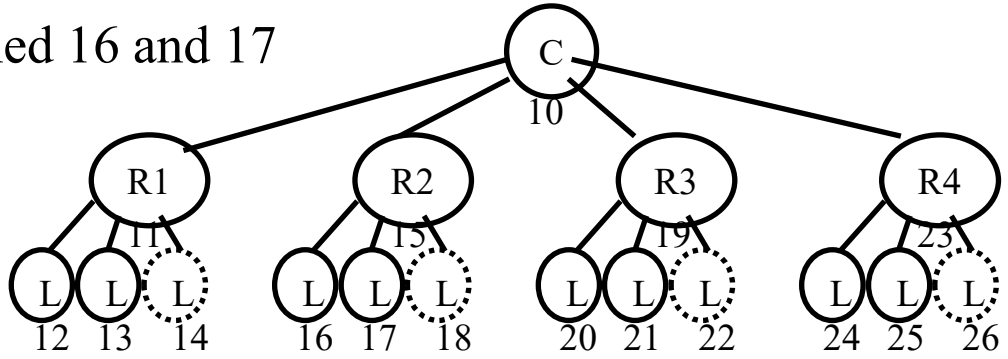
Student Questions

Distributed Scheme Example (Cont)

- Assume the address of coordinator is 10 (decimal)
- Address of R1 = 10+1 = 11
- Address of R2 = 10+1+S(0) = 11+4=15
- Address of R3 = 10+1+2*S(0) = 11+8 = 19
- Address of R3 = 10+1+3*S(0) = 11+12 =23
- Routers R1-R4 compute S(1):

$$S(1) = \frac{CR^{L-d-1} - 1 - C + R}{R - 1} = \frac{3 \times 4^{2-1-1} - 1 - 3 + 4}{4 - 1} = 1$$

- Children of R1 are assigned 12 and 13
- Children of R2 are assigned 16 and 17



Student Questions

Stochastic Address Assignment

- Parent draws a 16 bit random number between 0 and 2^{16}-1 and assigns it to a new child. A new number is drawn if the result is all-zero (null) or all-one (broadcast). So the assigned address is between 1 and 2^{16}-2.
- Parent then advertises the number to the network
- If another node has that address an address conflict message is returned and the parent draws another number and repeats
- There is no need to pre-limit # of children or depth

Student Questions

Zigbee Routing

1. Ad-Hoc On-Demand Distance Vector (**AODV**)
2. Dynamic Source Routing (**DSR**)
3. Tree Hierarchical Routing
4. Many-to-one routing

Note: Zigbee does not use DSR. It is presented here for completeness.

Student Questions

AODV

- Ad-hoc On-demand Distance Vector Routing
- On-demand ⇒ Reactive ⇒ Construct a route when needed
- Avoids unnecessary computations if no traffic
- Source broadcasts Route-Request (RREQ) command to all its neighbors containing source, destination, broadcast ID
- Each node determines if this is a new request or if this copy has a lower cost. If yes, it makes a "reverse route" entry for the source in its table w previous node as the optimal reverse path.
- The node then checks if it has a route to the destination. If yes, it sends "route-reply" to the source. Otherwise, it forwards the request to all its neighbors except where it came from.
- When the source receives a "route-reply" it selects the lowest cost path and sends the packet
- If a node cannot forward the packet, it sends a "Route Error" back to the source which will re-initate route discovery.

Student Questions

- Does this route error happen when a node in the lowest cost path drops off between the route reply and the sending of the packet? Or are there other reasons that can cause a route error?

Yes.

AODV Routing

- **Routing Table**: Path is not stored. Only next hop.
  - Entry = <destination, next node, "sequence #" (timestamp)>
- **Route Discovery**: Flood a **route request (RREQ)** to all neighbors. Neighbors broadcast to their neighbors

Src Addr	Req ID	Dest Addr	Src Seq #	Dest Seq #	Hop Count

- Request ID is the RREQ serial number. Used to discard duplicates.
  Source sequence # is a clock counter incremented when RREQ is sent.
  Destination sequence # is the most recent sequence from the destination that the source has seen. Zero if unknown.

Student Questions

AODV Routing (Cont)

- Intermediate nodes can reply to RREQ only if they have a route to destination with higher destination sequence #
- ***Route reply*** **(RREP)** comes back "unicast" on the reverse path

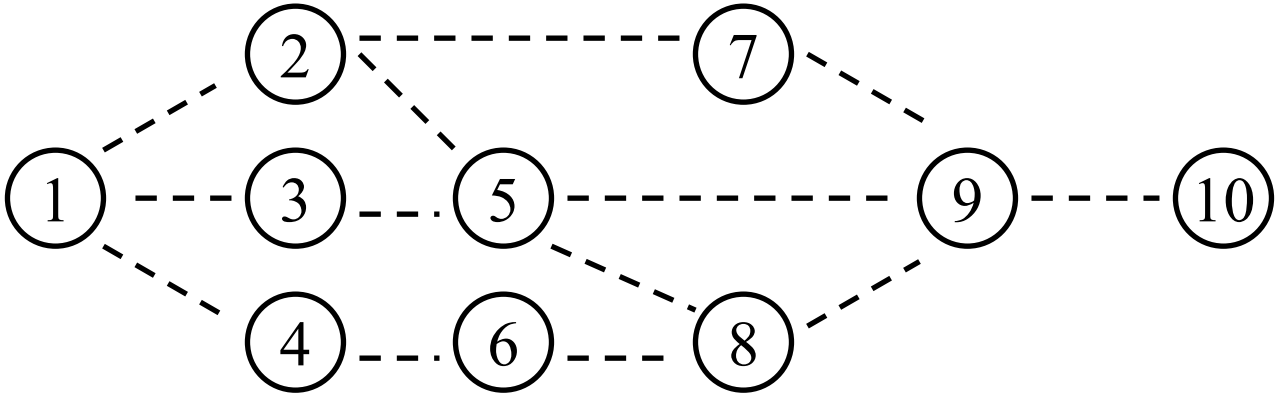
Src Addr	Dest Addr	Dest Seq #	Hop Count	Life Time

- Destination Sequence # is from Destination's counter
  Lifetime indicates how long the route is valid
- Intermediate nodes record node from both RREP and RREQ if it has a lower cost path ⇒ the reverse path
- Backward route to Destination is recorded if sequence number is higher or if sequence number is same and hops are lower
- Old entries are timed out
- AODV supports only symmetric links

Student Questions

AODV Routing: Example

- Node 1 broadcasts RREQ to 2, 3, 4:
  "*Any one has a route to 10 fresher than 1. This is my broadcast #1*"
- Node 2 broadcasts RREQ to 1, 5, 7
- Node 3 broadcasts RREQ to 1, 5
- Node 4 broadcasts RREQ to 1, 6



Student Questions

AODV Example (Cont)

Pkt # In	Pkt # Out	From	To	Message	Req ID	Src Seq #	Dest Seq #	Hops	Action at Receipient	New Table Entry Dest	Seq	Hops	Next
	1	1	2	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1
	2	1	3	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1
	3	1	4	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1
1	4	2	1	RREQ	1	1	1	2	Duplicate Req ID. Discard				
1	5	2	7	RREQ	1	1	1	2	New RREQ. Broadcast	1	1	2	2
1	6	2	5	RREQ	1	1	1	2	New RREQ. Broadcast	1	1	2	2
2	7	3	1	RREQ	1	1	1	2	Duplicate ID. Discard				
2	8	3	5	RREQ	1	1	1	2	Duplicate ID. Discard				
3	9	4	1	RREQ	1	1	1	2	Duplicate ID. Discard				
3	10	4	6	RREQ	1	1	1	2	New RREQ. Broadcast	1	1	2	4
5	11	7	2	RREQ	1	1	1	3	Duplicate ID. Discard				
5	12	7	9	RREQ	1	1	1	3	New RREQ. Broadcast	1	1	3	7
6	13	5	3	RREQ	1	1	1	3	Duplicate ID. Discard				
6	14	5	2	RREQ	1	1	1	3	Duplicate ID. Discard				
6	15	5	9	RREQ	1	1	1	3	Duplicate ID. Discard				
6	16	5	8	RREQ	1	1	1	3	New RREQ. Broadcast	1	1	3	5
10	17	6	4	RREQ	1	1	1	3	Duplicate ID. Discard				
10	18	6	8	RREQ	1	1	1	3	Duplicate ID. Discard				
12	19	9	8	RREQ	1	1	1	4	Duplicate ID. Discard				
12	20	9	5	RREQ	1	1	1	4	Duplicate ID. Discard				
12	21	9	7	RREQ	1	1	1	4	Duplicate ID. Discard				
12	22	9	10	RREQ	1	1	1	4	New RREQ. Respond	1	1	4	9
16	23	8	6	RREQ	1	1	1	4	Duplicate ID. Discard				
16	24	8	5	RREQ	1	1	1	4	Duplicate ID. Discard				
16	25	8	9	RREQ	1	1	1	4	Duplicate ID. Discard				
22	26	10	9	RREP	1	1	6	1	New RREP. Record and forward	10	6	1	10
26	27	9	7	RREP	1	1	6	2	New RREP. Record and forward	10	6	2	9
27	28	7	2	RREP	1	1	6	3	New RREP. Record and forward	10	6	3	7
28	29	2	1	RREP	1	1	6	4	New RREP. Record and forward	10	6	4	2

← Table entry at 2 for node 1

← Table entry at 4 for node 1

← Table entry at 9 for node 10

← Table entry at 2 for node 10

Student Questions

- What is the packet number "in" doing?

So you can co-relate it with packet#-out and follow the path of a packet.

- "Can you go over the table again? I was following up to where table at 10 is updated, but not quite after this part. Especially on how the time count is 6.

6 happens to be the sequence # at 10 at the time. It is arbitrary.

- Also, what does the first column Pkt# In mean?

See above.

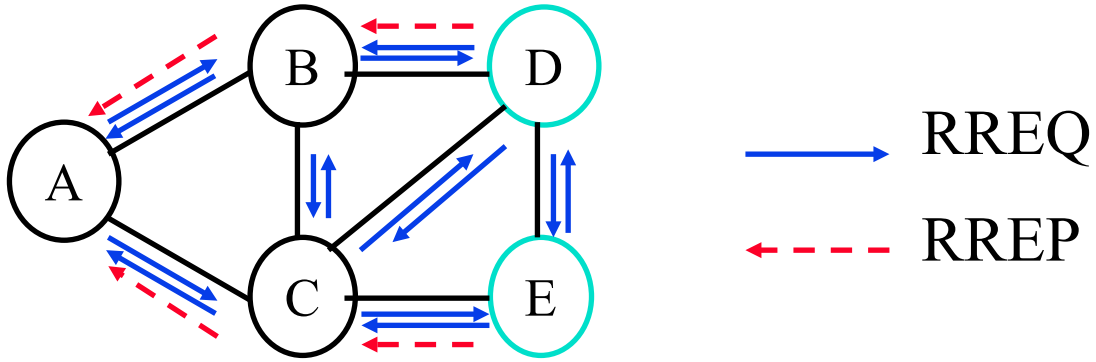
Multicast Route Discovery

- Similar to unicast route discovery
- If a node receives an RREQ but is not a member of the group or does not have the route to any member of the group, it creates a reverse-route entry and broadcasts the request to other neighbors
- If the node is a member of the group, it sends a RREP message to the source and forwards to other neighbors. Intermediate nodes make a note of this and set up a forward path

Student Questions

Multicast Discovery Example

- D and E are members. B and C are not.
- A concludes that the paths are ABD and ACE



Student Questions

Route Maintenance in AODV

- Each node keeps a list of active neighbors (replied to a hello within a timeout)
- If a link in a routing table breaks, all active neighbors are informed by "Route Error (RERR)" messages
- RERR is also sent if a packet transmission fails
- RERR contains the destination sequence # that failed
- When a source receives an RERR, it starts route discovery with that sequence number.
- Disadvantage: Intermediate nodes may send more up-to-date but still stale routes.
- Ref: RFC 3561, July 2003

Student Questions

Dynamic Source Routing (DSR)

- On-Demand (reactive) routing using "Source Route"
- Source Route = List of routers along the path in the packet.
- **Routing database**: Complete route to recent destinations
- Each entry has an expiration period and is timed out
- If a route is not available, send "*route request*" to all neighbors

Src Addr	Broadcast 255...255	RREQ	Req ID	Dest Addr	Route Record

- Each neighbor adds itself to the route in the request and forward to all its neighbors (only first receipt). Does not change source address.
- If a node knows the route it appends the rest of the route and returns the "*route reply (RREP)*"
- RREP goes back along the recorded path
- All nodes record paths in RREP and RREQ. Multiple routes cached.

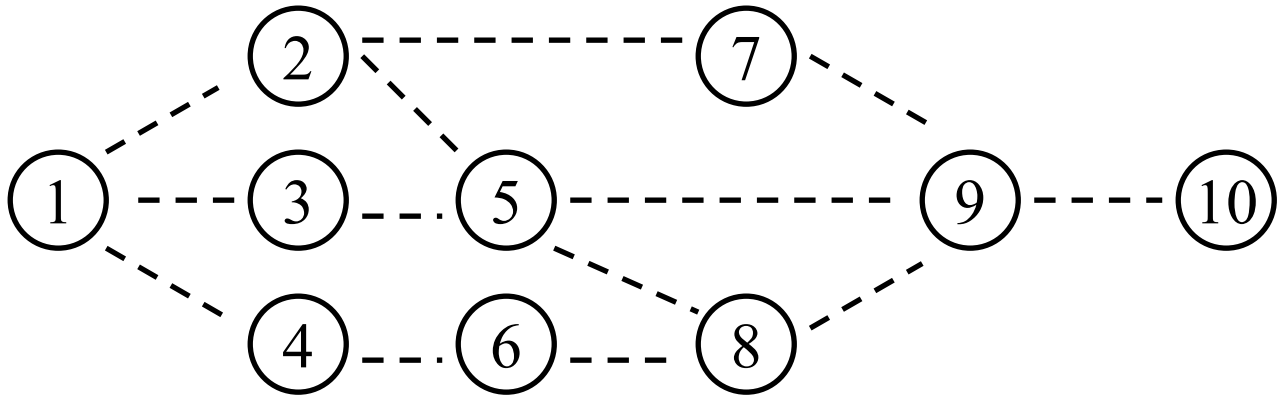
Student Questions

- So would the RREP be the same packet with source and destination address flipped?

Almost yes. The packet type may also need to be changed from request to reply.

DSR: Example

- Node 1 sends RREQ to 2, 3, 4:
  "*Any one has a route to 10*"
- Nodes 2 send RREQ to 5, 7. Note: RREQ not sent to 1.
- Node 3 sends RREQ to 5
- Node 4 sends RREQ to 6



Student Questions

DSR Example (Cont)

Pkt # In	Pkt # Out	From Node	To Node	Message Type	Req ID	Hops	Action at Receipient	Route Record in Packet
	1	1	2	RREQ	1	1	New RREQ. Record and forward	1-2
	2	1	3	RREQ	1	1	New RREQ. Record and forward.	1-3
	3	1	4	RREQ	1	1	New RREQ. Record and forward.	1-4
1	4	2	5	RREQ	1	2	New RREQ. Record and forward.	1-2-5
1	5	2	7	RREQ	1	2	New RREQ. Record and forward.	1-2-7
2	6	3	5	RREQ	1	2	Duplicate ID. Same hops. Record and forward.	1-3-5
3	7	4	6	RREQ	1	2	New RREQ. Record and forward.	1-4-6
4	8	5	8	RREQ	1	3	New RREQ. Record and forward.	1-2-5-8
4	9	5	9	RREQ	1	3	New RREQ. Record and forward.	1-2-5-9
5	10	7	9	RREQ	1	3	New RREQ. Same hops. Record and forward.	1-2-7-9
6	11	5	8	RREQ	1	3	Duplicate ID. Longer Path. Discard.	1-3-5-8
6	12	5	9	RREQ	1	3	New RREQ. Record and forward.	1-3-5-9
7	13	6	8	RREQ	1	3	New RREQ. Same hops. Record and forward.	1-4-6-8
8	14	8	6	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-5-8-6
8	15	8	9	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-5-8-9
9	16	9	8	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-5-8-9
9	17	9	7	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-5-9-7
9	18	9	10	RREQ	1	4	New RREQ. Respond through route 10-9-5-2-1	1-2-5-9-10
10	19	9	10	RREQ	1	4	New RREQ. Respond through route 10-9-7-2-1	1-2-7-9-10
10	20	9	8	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-7-9-8
10	21	9	5	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-7-9-5
12	22	9	10	RREQ	1	4	New RREQ. Respond through route 10-9-5-3-1	1-3-5-9-10
12	23	9	8	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-3-5-9-8
12	24	9	7	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-3-5-9-7
13	25	8	5	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-4-6-8-5
13	26	8	9	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-4-6-8-9
18	27	10	9	RREP	1	1	Record and forward along return path	10-9 (1-2-5-9-10)
19	28	10	9	RREP	1	1	Record and forward along return path	10-9 (1-2-7-9-10)
22	29	10	9	RREP	1	1	Record and forward along return path	10-9 (1-3-5-9-10)
27	30	9	5	RREP	1	2	Record and forward along return path	10-9-5 (1-2-5-9-10)
28	31	9	7	RREP	1	2	Record and forward along return path	10-9-7 (1-2-7-9-10)
29	32	9	5	RREP	1	2	Record and forward along return path	10-9-5 (1-3-5-9-10)
30	33	5	2	RREP	1	3	Record and forward along return path	10-9-5-2 (1-2-5-9-10)
31	34	7	2	RREP	1	3	Record and forward along return path	10-9-7-2 (1-2-7-9-10)
32	35	5	3	RREP	1	3	Record and forward along return path	10-9-5-3 (1-3-5-9-10)
33	36	2	1	RREP	1	4	Record and forward along return path	10-9-5-2-1 (1-2-5-9-10)
34	37	2	1	RREP	1	4	Record and forward along return path	10-9-7-2-1 (1-2-7-9-10)
35	38	3	1	RREP	1	4	Record and forward along return path	10-9-5-3-1 (1-3-5-9-10)

Student Questions

- Is the slide updated in the 2020 version? I don't understand why packet 18 has 1-2-5-9-7 in Route Record in Packet field. Can we go over the table again when the packet reaches node 10?

You are right. The record in packet 18 should be 1-2-5-9-10. Now it has been corrected.

Route Maintenance in DSR

- If a transmission fails, route error (RERR) is sent to the source. It contains hosts at both ends of the link.
- Intermediate nodes remove or truncate all routes with that link.
- Source may re-initate the route discovery.
- Caching multiple routes results in a faster recovery but the routes may be stale resulting in cache poisoning at other nodes.
- Not suitable for high-mobility environments.
- Source-route overhead in each packet.
- Ref: RFC 4728, February 2007

Student Questions

- Can you explain how cache poisoning may occur?

AODV vs. DSR

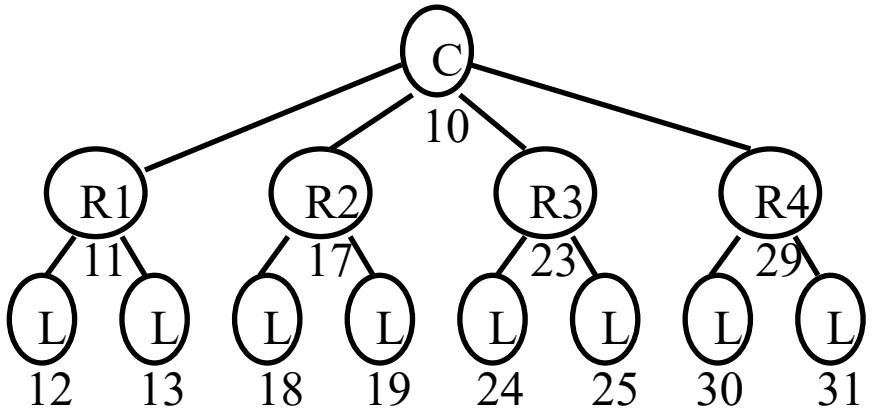
- In DSR a single RREQ can result in routes to several destination
- In DSR RERR messages are sent to the source not broadcast ⇒ Many nodes are unaware of failure
- In DSR, route discovery is delayed until all cached entries have been tried ⇒ Not good for high mobility

Feature	DSR	AODV
Routing Table	Route	Next Hop
Packet	Route	No route
Replies	Multiple	First only
Route Deletion	Fast Local	Slow Global

Student Questions

Tree Hierarchical Routing

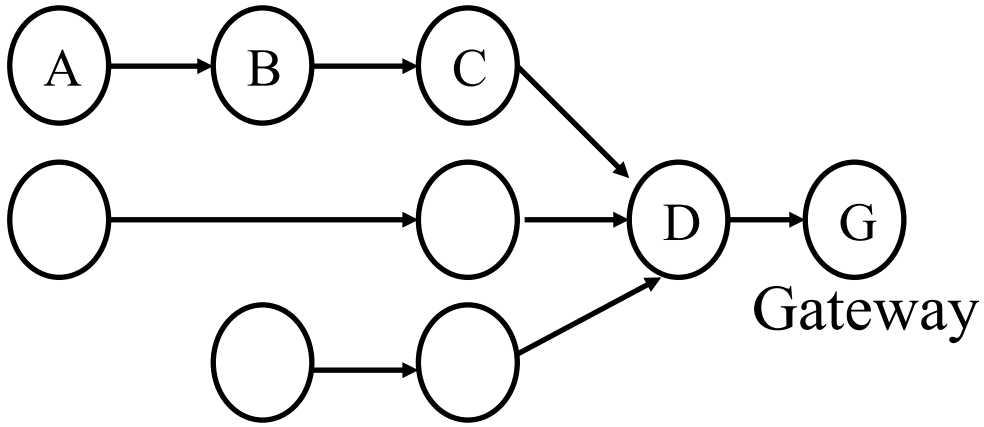
- All leaf nodes send the packet to their parent
- Each parent checks the address to see if it is in its subrange.
  - If yes, it sends to the appropriate child.
  - If not, it sends to its parent
- Example: A12 to A30. A12 → R1 → Coordinator → R4 → A30



Student Questions

Many-to-One Routing

- Used for sensor data collection. All data goes to a concentrator or a gateway
- Gateway has a large memory and can hold complete routes to all nodes
- But each node only remembers the next hop towards gateway



Student Questions

Zigbee RF4CE

- Radio Frequency for Consumer Electronics (RF4CE) consortium developed a protocol for remote control using wireless (rather than infrared which requires line of sight)
- RF4CE merged with Zigbee and produced Zigbee RF4CE protocol
- Operates on channels 15, 20, and 25 in 2.4 GHz
- Maximum PHY payload is 127 bytes
- Two types of devices: Remotes and Targets (TVs, DVD Player,…)
- **Status Display**: Remote can show the status of the target
- **Paging**: Can locate remote control using a paging button on the target
- **Pairing**: A remote control works only with certain devices

Student Questions

Zigbee 2030.5

- Formerly known as "Zigbee Smart Energy 2"
- Monitor, control, automate the delivery and use of energy and water
- Adds plug-in vehicle charging, configuration, and firmware download
- Developed in collaboration with other smart grid communication technologies: HomePlug, WiFi, …
- IP based ⇒ Incompatible with previous Zigbee

Student Questions

Zigbee IP

- Uses standard IPv6 frame format.
  ⇒ Allows connecting sensors directly to Internet w/o gateways
- Uses 802.15.4 PHY, MAC and ZigBee 2030.5
- IPv6 headers are compressed using **6LowPAN**
- **RPL** Routing to discover topology
- All Internet protocols: UDP, TCP, HTTP, … can be used
- Multicast forwarding and Service discovery using multicast DNS (mDNS) and DNS Service Discovery (DNS-SD)
- Security using standard protocols: TLS (Transport Layer Security), EAP (Extensible Authentication Protocol), PANA (Protocol for carrying Authentication for Network Access)
- Not compatible with other versions of Zigbee since they use a different network layer frame format
  ⇒ Need a gateway between Zigbee and Zigbee IP.

Student Questions

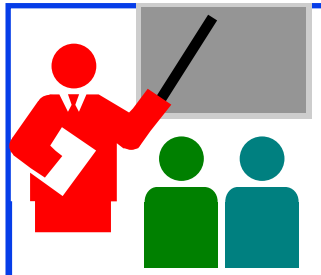
Ref: Zigbee Alliance, "Zigbee IP and 920IP," https://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeeip/

Z-Wave

- No relationship to Zigbee but competes with it in many applications and so often confused with it
- Search for Zigbee devices on Amazon shows many products that support only Z-Wave not Zigbee
- Originally a proprietary protocol developed for remote control. Now used for IoT.
- Now standardized by Z-Wave Alliance
- Uses 915/868 MHz band
- Many IoT hubs support Z-Wave along with Zigbee

Student Questions

Ref: Wikipedia, "Z-Wave," https://en.wikipedia.org/wiki/Z-Wave
Ref: Z-Wave Alliance, https://z-wavealliance.org/



Summary

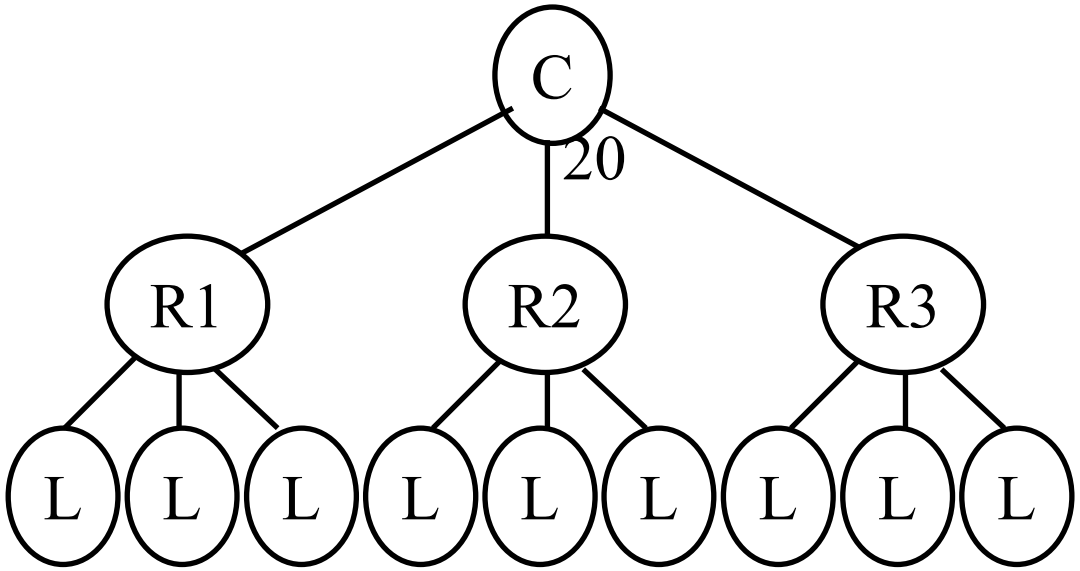
1. Zigbee is an IoT protocol for sensors, industrial automation, remote control using IEEE 802.15.4 PHY and MAC
2. Zigbee PRO supports stochastic addressing, many-to-one routing, fragmentation, and mesh topologies.
3. A number of application profiles have been defined with control and management provided by ZDOs.
4. Application Support layer provides data and command communication between application objects
5. Network layer provides addressing and routing. Addressing can be assigned using distributed or stochastic schemes. Routing is via AODV, DSR, Tree Hierarchical, or many-to-one routing.
6. Zigbee RF4CE and Zigbee SEP2 are Zigbee protocols designed specifically for remote control and smart grid, respectively.

Student Questions

- ❑ I think it would be beneficial to go over slides 3-6, as the delayed audio made it a bit more difficult to follow.

Slides were discussed 2,4,5,6,3 but inserted 2,3,4,5,6. A corrected version has been uploaded.

Homework 13A

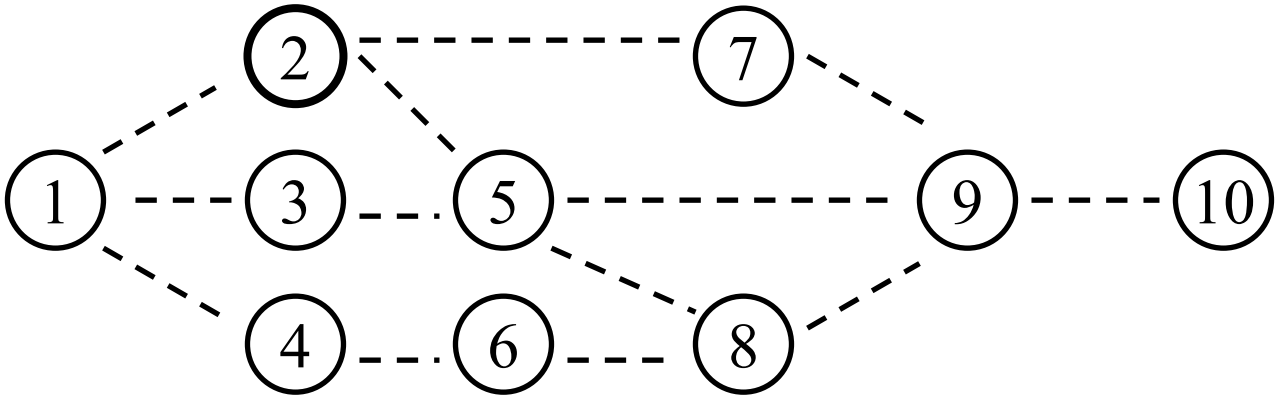


- Assuming that IEEE 802.15.4 network is being planned with a maximum of 5 children per node to a depth of 2 levels and maximum 4 routers. Compute sub-ranges to be assigned to each router and the addresses assigned to each node in the network assuming the coordinator has an address of 20.

Student Questions

Homework 13B

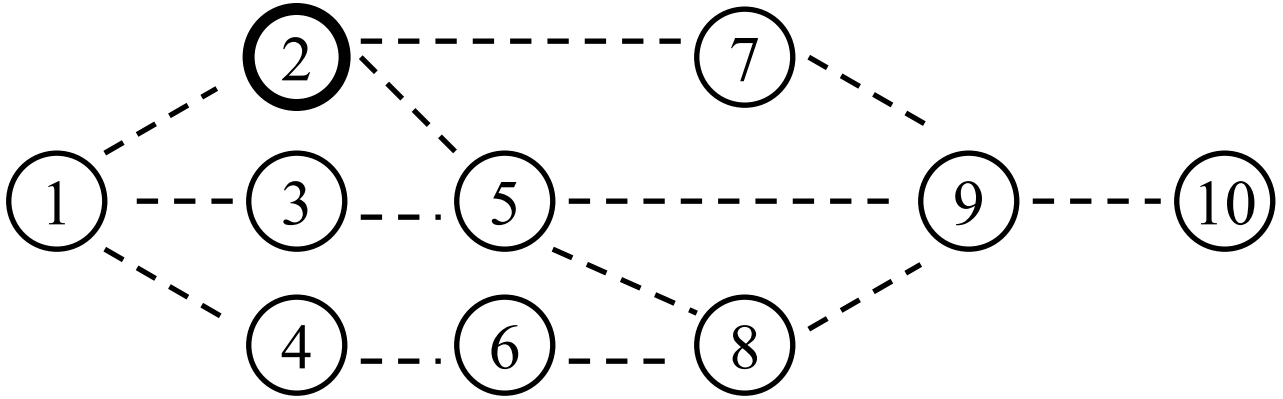
- Write the sequence of messages that will be sent in the following network when node 2 tries to find the path to node 10 in the AODV example.



Student Questions

Homework 13C

- Write the sequence of messages that will be sent in the following network when node 2 tries to find the path to node 10 in the DSR example.



Student Questions

Reading List

- A. Elahi and A. Gschwender, "Zigbee Wireless Sensor and Control Network," Prentice Hall, 2009, 288 pp., ISBN:0137134851, Safari Book, Chapters 2, 5, 6, 9
- K. Garg, "Mobile Computing: Theory and Practice," Pearson, 2010, ISBN: 81-3173-166-9, 232 pp., Safari Book, Sections 6.5-6.7
- R. Jain, "Networking Protocols for Internet of Things," (6LowPAN and RPL)," http://www.cse.wustl.edu/~jain/cse570-13/m_19lpn.htm

Student Questions

Related Wikipedia Pages

- http://en.wikipedia.org/wiki/Zigbee
- http://en.wikipedia.org/wiki/Ad_hoc_On-Demand_Distance_Vector_Routing
- http://en.wikipedia.org/wiki/Dynamic_Source_Routing
- http://en.wikipedia.org/wiki/Source_routing
- http://en.wikipedia.org/wiki/Loose_Source_Routing

Student Questions

References

1. D. A. Gratton, "The Handbook of Personal Area Networking Technologies and Protocols," Cambridge University Press, 2013, 424 pp., ISBN:9780521197267, Safar Book.
2. O. Hersent, et al., "The Internet of Things: Key Applications and Protocols," Wiley, 2012, 370 pp., ISBN:978111994350, Safari Book.
3. N. Hunn, "Essentials of Short Range Wireless," Cambridge University Press, 2010, 344 pp., ISBN:9780521760690, Safari book.
4. D.Gislason, "Zigbee Wireless Networking," Newnes, 2008, 288 pp., ISBN:07506-85972, Safari book.
5. S. Farahani, "Zigbee Wireless Network and Transceivers," Newnes, 2008
6. J. Gutierrez, E. Gallaway, and R. Barrett, "Low-Rate Wireless Personnel Area Networks," IEEE Press Publication, 2007
7. H. Labiod, H. Afifi, C. De Santis, "Wi-Fi, Bluetooth, Zigbee and WiMax," Springer, Jun 2007, 316 pp., ISBN:1402053967.
8. I. Guvenc, et al., "Reliable Communications for Short-Range Wireless Systems," Cambridge University Press, March 2011, 426 pp., ISBN: 978-0-521-76317-2, Safari Book

Student Questions

References (Cont)

- Zigbee Alliance Technical Documents, http://www.zigbee.org/Products/TechnicalDocumentsDownload/tabid/237/Default.aspx
- Zigbee Alliance Whitepapers, http://www.zigbee.org/LearnMore/WhitePapers/tabid/257/Default.aspx
- Zigbee Alliance, Zigbee Specification Document 053474r17, 2008
- Daintree Network, "Comparing Zigbee Specification Versions," www.daintree.net/resources/spec-matrix.php
- "How Does Zigbee Compare with Other Wireless Standards?" www.stg.com/wireless/Zigbee-comp.html

Student Questions

References (Cont)

- Zigbee IEEE 802.15.4 Summary, http://www.eecs.berkeley.edu/~csinem/academic/publications/zigbee.pdf
- I., Poole, "What exactly is . . . Zigbee?", Volume 2, Issue 4, Pages: 44-45, IEEE Communications Engineer, 2004, http://ieeexplore.ieee.org/iel5/8515/29539/01340336.pdf?tp=&arnumber=1340336&isnumber=29539
- "Zigbee starts to buzz", Volume 50, Issue 11, Pages: 17-17, IEE Review, Nov. 2004 http://ieeexplore.ieee.org/iel5/2188/30357/01395370.pdf?tp=&arnumber=1395370&isnumber=30357
- C. Evans-Pughe,"Bzzzz zzz [Zigbee wireless standard]", Volume 49, Issue 3, Pages:28-31, IEE Review, March 2003
- Craig, William C. "Zigbee: Wireless Control That Simply Works," Zigbee Alliance, 2003

Student Questions

Acronyms

- AODV Ad-Hoc On-Demand Distance Vector
- APS Application Support Sublayer
- APSDE Application Support Sublayer Data Entity
- APSME Application Support Sublayer Management Entity
- CSMA/CA Carrier Sense Multiple Access
- DNS Domain Name System
- DSR Dynamic Source Routing
- DVD Digital Video Disc
- EP End Point
- GHz Giga Hertz
- ID Identifier
- IEE Institution of Electrical Engineers (UK) now IET
- IEEE Institution of Electrical and Electronic Engineers
- IET Institution of Engineering and Technology
- IoT Internet of Things
- IP Internet Protocols

Student Questions

Acronyms (Cont)

- ISM Instrumentation, Scientific, and Medical
- kB Kilo byte
- MAC Media Access Control
- MHz Mega Hertz
- NPDU Network Protocol Data Unit
- NPDU Network Service Data Unit
- PHHC Personal, Home, and Hospital Care
- PHY Physical Layer
- RF4CE Radio Frequency for Consumer Electronics
- RFC Request for Comment
- RFID Radio Frequency ID
- RREP Route Reply
- RREQ Route Request
- UWB Ultra Wide-Band
- WiFi Wireless Fidelity

Student Questions

Acronyms (Cont)

- WiMAX Worldwide Interoperability for Microwave Access
- WWAN Wireless Wide Area Network
- ZDO Zigbee Device Object

Student Questions

Scan This to Download These Slides

Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse574-20/j_13zgb.htm

Student Questions

Announcements:

Module 14 Q&A will be discussed on Monday 11/9. Homework 14 be due on Monday, 11/16. The day of the mid-term exam 2.
It would be best to do the homework early and ask questions on Wednesday 11/11. Should we change the deadline to 11/11?

Related Modules

CSE567M: Computer Systems Analysis (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw

Recent Advances in Networking (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw

Student Questions